UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/658,246	09/08/2003	Stephen Zizzi	M000-P03098US	4125

33356 7590 01/18/2006

SoCAL IP LAW GROUP LLP
310 N. WESTLAKE BLVD. STE 120
WESTLAKE VILLAGE, CA 91362

EXAMINER	
DARROW, JUSTIN T	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 01/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/658,246	ZIZZI, STEPHEN	
	Examiner	Art Unit	
	Justin T. Darrow	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *13,15-19,21,22 and 29-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *13,15-19,21,22 and 29-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-45 have been presented for examination. Claims 1-12, 14, 20, and 23-28 have been canceled, claims 13, 15-19, 21, and 22 have been amended, and new claims 29-45 have been added in a preliminary amendment filed 05/13/2005. Claims 13, 15-19, 21, 22, and 29-45 have been examined.

Priority

2. Acknowledgment is made that the instant application is a continuation-in-part of Application No. 09/259,991, filed 03/01/1999, now U.S. Patent No. 6,981,141 B1, which is a continuation-in-part of Application No. 09/074,191, filed 05/07/1998, now U.S. Patent No. 6,185,681 B1.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 01/09/2004 was filed before the mailing date of the first Office action on the merits. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

4. The disclosure is objected to because of the following informalities:

delete "1999;" in page 1, ¶ [0002], line 2 and replace with --1999, now U.S. Patent No. 6,981,141,--.

Appropriate correction is required.

Claim Objections

5. Claim 33 is objected to because of the following informalities:

delete "record" in line 5 and replace with --recorded--. Appropriate correction is required.

6. Claim 40 is objected to because of the following informalities:

delete "record" in line 5 and replace with --recorded--. Appropriate correction is required.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claim 13 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 13 recites the limitation "electronic document management system" in line 4. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 15-19, 21, 22, and 29-45 are rejected under 35 U.S.C. 102(e) as being anticipated by Brundrett et al., U.S. Patent No. 6,249,866 B1.

As per claims 29 and 33, Brundrett et al. illustrates a process and a computer program product for decrypting documents comprising:

providing plural documents having respective names (see column 4, lines 13-17; figure 1, items 44_1-44_n; a number of files with names in the form of information identifying the data streams belonging to the respective files);

providing a crypto server for causing documents to be decrypted (see column 7, line 67; column 8, lines 1-7; figure 2, item 50; an electronic file system (EFS) service with networking and interface capability for file distribution that interfaces with a Cryptography application programming interface (API) for decrypting encrypted files);

providing a first table (see column 11, lines 25-27; figure 6, item 96; information of the key context arranged in tabular form) having

names of encrypted documents (see column 11, lines 20-30; figure 6, items 94_1, 94_3, and 94_n and 96_1, 96_2, and 96_n; key contexts labeled with name consisting of the filename F and the order of the document in the file, numeral m);

for each of the names of encrypted documents in the table, a key name associated with a decryption key value for the encrypted document (see column 6, lines 26-36; figure 2, items 46 and 48; figure 7, items 98_1, 98_8, 98_{13}, and 98_n; the Encrypting File System Runtime Library (FSLTR) maintains a context buffer in the form of a table indicating key names F1, F8, F13, and Fn);

detecting an open command for a given document issuing from a user of an application program using a user input device (see column 4, lines 43-48; receiving an I/O request packet to open a file; see column 3, lines 57-61; figure 1, items 34 and 36; where the I/O circuitry is connected to a user input device; see column 4, lines 36-41; figure 2, items 46 and 48; for applications such as opening, reading, writing, and appending);

in response to the open command, the crypto server using the first table to determine if the given document should be decrypted (see column 6, lines 10-14 and 26-36; figure 2, items 46 and 48; figure 7, items 98_1, 98_8, 98_{13}, and 98; the Encrypting File System Runtime Library (FSLTR) maintains a context buffer in the form of a table indicating to the Encrypting File System (EFS) driver which blocks are to be decrypted if the request is a file open request on an existing file);

if the given document should be decrypted (see column 6, lines 15-18; when file encryption key is extracted from the metadata connoting that the file should be decrypted), then

retrieving the key name associated with the name of the given document from the first table (see column 6, lines 36-39; figure 2, item 46; the Encrypting File System (EFS) driver can call in to access the encryption meta data); and

retrieving the decryption key value associated with the key name from a second table, having at least one decryption value causing the given document to be decrypted (see column 17, lines 16-23; figure 2, items 28 and 46; figure 6, items 96_1, 96_2, and 96_n; the encryption driver is provided by the NTFS with the encryption context to decrypt the blocks).

As per claim 15, Brudrett et al. further points out:

the user submitting to an access module for user authentication (see column 11, lines 5-10; figure 4, items 84 and 86; the user provides a private key to an extraction mechanism);

if the access module does not authenticate the user, determining that the document should not be decrypted (see column 11, lines 5-10; figure 4, item 60; if there is no match found between the private key provided by the user and the value used to properly decrypt the file encryption key (FEK), then the file is not decrypted);

else, the crypto server retrieving the decryption key value associated with the key name (see column 10, lines 40-42; figure 3, items 70 and 82; where the file encryption key (FEK) is associated with a list of names of encrypted file encryption keys stored with the file in a Data Recovery Field (DRF)) and the user (see column 10, lines 10-15; figure 3, items 60 and 72; where the file encryption key is encrypted with a public key of the user).

As per claim 16, Brudrett et al. additionally specifies:

providing a data reader device for reading user identification and decryption key values from a portable storage device (see column 18, lines 46-49; smart cards and floppy disks for storing keys; see column 10, lines 20-23; including the private key identifying a particular user),

where the user presents the portable data storage device to the data reader device (see column 11, lines 5-10; figure 4, items 50 and 86; feeding the user's private key from the smart card to an extraction mechanism in the encrypting file system (EFS)),

wherein the access module utilizes information stored in the portable data storage device to authenticate the user (see column 11, lines 5-10; figure 4, item 60; where the user is authenticated when a match is found that the user's private key properly decrypts the file encryption key FEK), and the decryption key value associated with the user is stored in the portable data storage device (see column 18, lines 46-49; the keys may be alternatively stored on smart cards and/or floppy disks).

As per claim 17, Brundrett et al. then specifies:

that the portable storage device comprises a smart card (see column 18, lines 46-49; smart cards for storing keys; see column 10, lines 20-23; including the private key identifying a particular user).

As per claim 18, Brundrett et al. additionally explains:

that the portable storage device comprises the user identification (see column 10, lines 20-23; figure 4, item 84; storing the private portion of a user's key pair on a secure storage device),

wherein the access module utilizes unique information about the user for authentication (see column 11, lines 5-10; figure 4, item 60; where the user is authenticated when a match is found that the user's private key properly decrypts the file encryption key FEK), and

the decryption key value is derived from at least one characteristic of the user (see column 11, lines 5-10; figure 4, item 60; where the file encryption key FEK decrypted with the user's private key essentially results in the file encryption key FEK being derived from the user's private key as a characteristic of the user).

As pre claim 19, Brundrett et al. then points out:

providing a database including an indicator of whether the documents should be decrypted (see column 11, lines 20-33; figure 6, items 28, 94_1, and 96_1; a key context in the Windows NT® file system (NTFS) corresponding to a stream control block of a file maintaining information necessary to decrypt a file during reads from the disk);

where if the indicator in the database does not indicate that the given document is to be decrypted, determining that the document should not be decrypted (see column 11, lines 27-33; where only certain block documents in a large file are decrypted in accordance with the key context for specific readings from the disk).

As per claims 21 and 35, Brundrett et al. next discusses:

the process being performed in a general purpose computer having an operating system (see column 3, lines 43-45; figure 1, items 20 and 26; the computer includes an operating system),

wherein the operating system includes at least a part of an electronic document management system (see column 3, lines 47-49; figure 1, items 26 and 28; Windows NT® file system (NTFS) is associated with or included within the operating system).

As per claim 22, Brundrett et al. moreover shows:

a workstation (see column 3, lines 43-45; figure 1, item 20; a computer system),

a file server wherein the crypto server is disposed on the workstation (see column 7, line 67; column 8, lines 1-3; figure 1, items 50 and 58; an encrypting file system (EFS) interfacing with a cryptography application programming interface CryptoAPI).

As per claims 30 and 39, Brundrett et al. then describes:

that the decryption key value is related to an identity of the user (see column 10, lines 23-25; a user-password-derived key for decryption of the document).

As per claims 31 and 34, Brundrett et al. also mentions:

an algorithm selected from DES (see column 10, lines 5-9), and RSA (see column 10, lines 37-38).

As per claims 32 and 38, Brundrett et al. further discusses:

that the second table is stored in a smart card (see column 18, lines 33-49; mechanisms of key storage for encrypting file system (EFS) support can be stored on smart cards).

As per claim 36, Brundrett et al. additionally elaborates:

interfacing with plural cryptographic systems (see column 9, lines 21-29; EncryptFile and DecryptFile; column 9, lines 29-47; OpenRawFile and CloseRawFile are examples of cryptographic systems available to the encrypting filing system (EFS)).

As per claim 37, Brundrett et al. then points out:

obtaining the decryption key values from a portable data storage device (see column 18, lines 46-49; the keys may be alternatively stored on smart cards and/or floppy disks from which they are retrieved).

As per claim 40, Brundrett et al. illustrate a computer program product for causing a processor to

cause plural documents to be encrypted (see column 7, line 67; column 8, lines 1-3; figure 1, items 50 and 58; an encrypting file system (EFS) interfacing with a cryptographic application programming interface (CryptoAPI)), the documents having respective names recorded in a first table (see column 11, lines 20-30; figure 6, items 94_1, 94_3, and 94_n and 96_1, 96_2, and 96_n; key contexts labeled with name consisting of the filename F and the order of the document in the file, numeral m, arranged in tabular form),

the names of the encrypted documents (see column 11, lines 20-30; figure 6, items 94_1, 94_3, and 94_n and 96_1, 96_2, and 96_n; key contexts labeled with name consisting of the filename F and the order of the document in the file, numeral m)

for each of the names of encrypted documents in the table, a key name associated with an encryption key value for the encrypted document (see column 6, lines 26-36; figure 2, items 46 and 48; figure 7, items 98_1, 98_8, 98_{13}, and 98_n; the Encrypting File System Runtime Library (FSLTR) maintains a context buffer in the form of a table indicating key names F1, F8, F13, and Fn),

detect a close command for a given document issuing from a user of an application program using a user input device (see column 5, lines 32-34; a transparent encryption process where the user requests to write the data to non-volatile storage media; see column 9, lines 42-46; a CloseRawFile interface is provided that allows the user to close the file and a WriteRawFile interface that allows the user to write all the data to the file),

in response to the close command use the first table to determine if the given document should be encrypted (see column 9, lines 47-53; where the file control for encrypting the file must be verified to determine if the file is to be encrypted),

if the given document should be encrypted (see column 9, lines 54-57; if the metadata indicates that the document should be encrypted), then

retrieve the key name associated with the name of the given document from the first table (see column 11, lines 21-25; figure 6, items 94_1 and 96_1; obtaining a key context corresponding to the file),

retrieve the encryption key value associated with the key name from a second table, having at least one encryption key value and at least one key name respectively associated with a one of the encryption key values (see column 11, lines 25-27; figure 6, item 96; obtaining the key context maintaining information necessary to encrypt the file during writes to the disk),

cause the given document to be encrypted (see column 10, lines 5-9; figure 3, items 60, 64, 66, 68, and 70; the file data as plaintext is encrypted with the file encryption key FEK by the file encryption mechanism and written to an encrypted file).

As per claim 41, Brundrett et al. also mentions:

an algorithm selected from DES (see column 10, lines 5-9), and RSA (see column 10, lines 37-38).

As per claim 42, Brundrett et al. next discusses:

a general purpose computer (see column 3, lines 32-35; figure 1, item 20; the computer into which the encryption program is incorporated).

As per claim 43, Brundrett et al. additionally elaborates:

interfacing with plural cryptographic systems (see column 9, lines 21-29; EncryptFile and DecryptFile; column 9, lines 29-47; OpenRawFile and CloseRawFile are examples of cryptographic systems available to the encrypting filing system (EFS)).

As per claim 44, Brundrett et al. then points out:

obtaining the decryption key values from a portable data storage device (see column 18, lines 46-49; the keys may be alternatively stored on smart cards and/or floppy disks from which they are retrieved).

As per claim 45, Brundrett et al. further discusses:

that the second table is stored in a smart card (see column 18, lines 33-49; mechanisms of key storage for encrypting file system (EFS) support can be stored on smart cards).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Brundrett et al., U.S. Patent No. 6,249,866 B1 as applied to claim 29 above, and further in view of Chan, U.S. Patent No. 5,713,018 A.

Brundrett et al. discloses the process of decrypting documents of claim 29. However, this reference does not explicitly teach a SQL database, a SQL database server, nor a SQL database client.

Chan elaborates on:

an electronic database management system comprising a SQL database, a SQL database server, and a SQL database client in which an electronic document management system (see column 2, lines 35-61 and figure 1, items 130, 104, and 102; a client computer, an information server, and database management system with SQL interface procedures and responsive to SQL

statements), where the system detects an open command (see column 1, lines 53-57; SQL statements for reading data in a document to be opened).

Therefore, it would have been obvious to one of ordinary skill in the computer art at the time of the invention was made to combine the method of Brundrett et al. with the electronic database management system comprising a SQL database, a SQL database server, and a SQL database client of Chan to promote a standard interfacing language to facilitate upgrades with preventing system failures.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Johnson et al., U.S. Patent No. 5,694,472 A discloses an encryption file system in which the processing device authenticates the storage device to determine if the storage device is authorized to operate with the processing device.

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (571) 272-3801, and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is 571-273-8300. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to 571-273-8300 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-2100.

January 11, 2006

Justin Darrow

JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100